

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

Diabetes Technology Society

Standard for Connected Diabetes Device Security (DTSec)

December 28, 2015
Version 0.8

DTSEC-2015-08-000

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

31

32 **Legal Notice:**

33

34 *Diabetes Technology Society (DTS) organized the development of this version of the*
35 *Diabetes Technology Society Standard for Wireless Device Security (DTSec). As the*
36 *holder of the copyright in the Diabetes Technology Society Standard for Wireless*
37 *Device Security (DTSec), DTS retains the right to use, copy, distribute, translate or*
38 *modify DTSec as it sees fit.*

39

40

41

42

Foreword

43

44

45

46 This version of DTSec (v1.7) is a revised version based on suggestions from the
47 DTSec Steering Committee and Advisors. This standard and related Protection
48 Profiles, which are managed by the DTSec Working Group (DWG), consists of scope
49 of work, Protection Profile, and Assurance committees, all working under the
50 auspices of the Diabetes Technology Society. This draft document is not intended for
51 official use.

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

52
53

54 **Table of Contents**

55	Foreword.....	2
56	1. INTRODUCTION	4
57	Scope	5
58	ISO/IEC 15408.....	6
59	Protection Profiles and Security Targets	7
60	ISO 15408 Assurance Packages	8
61	2. ASSURANCE PROGRAM	10
62	Lab Accreditation.....	10
63	Product Certification	11
64	Evaluated Products List.....	11
65	Protection Profile and Security Target Approval	11
66	Assurance Maintenance Program	11
67		
68		

DRAFT

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

69

70 1. INTRODUCTION

71

72 The following section is non-normative, with the exception of statements that
73 include the word "***shall***" in boldface italics.

74

75 The purpose of DTSec is to establish a standard used to provide a high level of
76 assurance that electronic products deliver the security protections claimed by their
77 developers and required by their users. While this standard is initially targeted to
78 networked life-critical devices, such as insulin pump controllers, used in the
79 treatment of diabetes, there is nothing inherent in this standard that precludes its
80 application to any medical product or component contributing to the protection of
81 high value assets, resources, and functions. Indeed, while the Diabetes Technology
82 Society has a specific mission in diabetes-related electronic products, it is the
83 express intent of this standard's authors that it can provide foundational work for
84 effective cybersecurity standards across not only other medical device classes but
85 other connected devices and the broader "Internet of Things."

86

87 In order to meet the goal above, participants in the creation of this standard share
88 the following objectives:

89

- 90 1. Enhance the likelihood that security evaluations of critical medical products
91 are performed to high standards, including the ability to achieve highly
92 assured protection and an overall contribution towards enhanced safety,
93 privacy, and security for electronic product stakeholders, including product
94 manufacturers, regulators, patients, and caregivers;
- 95 2. Increase the availability of critical electronic products that have been
96 independently evaluated and certified to meet such high standards;
- 97 3. Reduce the use of ad-hoc, unreliable, and low assurance electronic product
98 development and evaluation methods that increase risk to electronic product
99 stakeholders;
- 100 4. Continuously improve the efficiency (cost and time) of the evaluation and
101 certification of critical electronic products.

102

103

104 Professional symposia that support DTSec:

105 [Diabetes Technology Society Annual Conference](#)

106 [MEDSec \(Medical Cybersecurity and Privacy: The Internet of Medical Things\)](#)

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

107

108 **Scope**

109

110 This section describes the scope of the DTSec standard.

111

112 Medical devices used for monitoring and managing diabetes provide life-saving
113 benefits to patients and effective implementation options to healthcare providers.
114 These devices include blood glucose monitors and continuous glucose monitors,
115 insulin pumps, pens and other insulin delivery devices, and closed loop artificial
116 pancreas systems. With ever-increasing connectivity and data exchange between
117 these diabetes devices, other devices (such as smart phones), and the Internet, there
118 is an increased risk to the safety and privacy of the patient and to the integrity of the
119 healthcare provider. The DTSec program calls for the specification of security
120 requirements for wireless diabetes devices and following the general framework of
121 establishing security standards for information and electronic systems (ISO/IEC
122 15408, described in the following section). These requirements are codified by the
123 use of Protection Profiles and Security Targets (explained later in this document),
124 but at a high level have the following objectives:

125

126 • To establish the general requirements for connected devices that
127 meet the balanced needs for security and clinical application.

128 • To identify possible and potential threats related to the various
129 components and interfaces of the connected devices, such as network,
130 storage, software, connected peer devices, and cryptography.

131 • To define a set of generalized requirements that apply to families of
132 similar devices (these are formed into the Protection Profile)

133 • To define a set of specific mandatory requirements, derived from the
134 generalized requirements, corresponding to specific connected-
135 diabetes device products and components (these requirements are
136 formed into the Security Target).

137 • To outline additional optional functional requirements for
138 manufacturers to consider to add to their toolbox for future
139 development.

140

141 In addition to security functional requirements, the Protection Profiles and Security
142 Targets specify assurance requirements to address the question of: how can I be
143 sure that a wireless diabetes device actually delivers the security claimed in the
144 functional requirements? Common assurance requirements are collected into an
145 assurance package, described in more detail later in this document, and formally
146 defined in the Protection Profiles and Security Targets themselves.

147

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

148 In addition to the program for creation and approval of security requirements
149 documents, this standard also defines the assurance program for evaluating and
150 certifying products against those requirements. The assurance program is defined
151 later in this document.

152
153 In summary, the DTSec scope includes a program for specifying security
154 requirements for wireless diabetes devices and a program for generating
155 independent assurance (by technical evaluation) that products meet the specified
156 requirements. The remainder of this standard document provides more detailed
157 information about these items and specific mandatory guidance for how this
158 standard is applied.

159

160 **ISO/IEC 15408**

161

162 To be effective for critical electronic devices, especially those that are network
163 connected and may be subject to remote malicious attack, security standards must
164 delve deeply into the processes and techniques for developing and deploying
165 security technologies that provide high assurance of protection. A consortium of
166 national governments came together in the mid 1990s to create a framework for
167 specifying security requirements - for any electronics product, software component,
168 or system - and evaluating vendor claims of conformance to the requirements. The
169 framework that was developed is ISO/IEC 15408, known informally as the Common
170 Criteria (CC), which remains the only internationally accepted, generally applicable
171 product security framework. CC has been utilized to specify a wide variety of
172 security functionality over almost two decades. Requirements are specified in two
173 dimensions: functional requirements cover security features of a product or
174 component, while assurance requirements provide the confidence those features
175 actually do what they claim. CC is a powerful, scalable framework that permits
176 comparability and consistency between the results of independent security
177 evaluations that follow the standard's methodology. CC assurance requirements can
178 be thought of as falling into two broad areas: product-independent, organizational
179 requirements (e.g. life-cycle processes, configuration management controls, a
180 process and common approach to design and specification, etc.) and product-
181 dependent requirements (e.g. design and requirements artifacts specific to a
182 particular system, functional test results, and vulnerability assessment).

183

184 Security functional requirements vary widely across products and product
185 components, depending on their threat profile. For example, the security functional
186 requirements for a wireless insulin controller may include:

187

- 188 • authentication to ensure the controller is only operated by authorized
189 users

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

- 190 • device and software authentication to ensure that only authentic,
191 trustworthy devices and their constituent software/firmware are
192 used to administer insulin
- 193 • data integrity and confidentiality to protect against corruption or
194 other unauthorized access to commands sent between controller and
195 pump
- 196 • data confidentiality to safeguard the personal data (privacy) of
197 patients and other persons
198

199 Protection Profiles and Security Targets

200
201 The CC provides for the creation of product-specific requirements specifications,
202 against which individual commercial products or product components are
203 evaluated. The two types of specifications are Protection Profiles (PP) and Security
204 Targets (ST). PPs are intended to generalize the requirements for a wide range of
205 similar products and represent the appropriate security and assurance
206 requirements for a class of devices derived from a technical community of clinical
207 and security experts. This enables the purchaser of a device to acquire a secure
208 product by specifying that the device meet the requirements of the PP rather than
209 detailing all requirements for each device purchase. STs, in contrast, provide specific
210 requirements for a specific product or component from a specific manufacturer. For
211 example, if there are numerous manufacturers of insulin pump controllers, all of
212 which have similar security requirements, then a PP can be authored by a technical
213 community of manufacturers and other stakeholders (e.g. caregivers, regulators,
214 independent cybersecurity experts) to cover insulin pump controllers. A
215 manufacturer can then tailor an ST from the PP. Evaluations are performed against
216 STs. PPs **shall** be authored by DWG and used when significant efficiency is to be
217 gained from a common security specification and to reduce the subsequent
218 resources required to develop derived STs.

219
220 The CC provides a large menu of common functional requirements, from which PP
221 and ST authors may choose. Whenever possible, requirements should be selected
222 from this menu. PP authors also have the freedom under the CC to define
223 “extended” requirements to address requirements not explicitly listed in the
224 standard. For example, embedded medical electronics may have requirements not
225 initially conceived by the CC standards authors targeting general IT systems. The
226 complete selection of requirements for PPs and STs must be carefully made based
227 on the device threat model, including the functional attack vectors (local/physical,
228 local network, wide-area network, supply chain, etc.) and the motivation and
229 sophistication of attackers to which the product’s security capabilities must be
230 resistant.
231

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

232 Security evaluation and certification performed under the auspices of this standard
233 **shall** utilize international standard ISO/IEC 15408:2009 (general framework and
234 specification of requirements) and ISO/IEC 18045:2005 (companion document to
235 ISO 15408, covering evaluation methodology).

236 **ISO 15408 Assurance Packages**

237
238 Assurance requirements can be grouped into a package that is reused across
239 different PPs and STs. Standards bodies and developers can create customized
240 assurance packages. For example, packages may vary the rigor of vulnerability
241 assessment, depending upon the reasonably expected magnitude of anticipated
242 threats threat (e.g. nation state vs. amateur hackers).

243
244 Each assurance requirement originates from a particular assurance component,
245 where each component includes a selection of related requirements in increasing
246 levels of rigor, corresponding to the needs of increasing assurance. DWG may create
247 a package that adopts more rigorous requirements for testing and vulnerability
248 assessment activities that are tightly coupled to device implementation. However,
249 because medical device manufacturers often follow a mature, high quality software
250 development life-cycle process, such as one compliant to IEC 62304, an
251 international and widely adopted standard for medical device software lifecycle
252 processes, compliance (and associated audit) to IEC 62304 may be used as a cost-
253 effective replacement for evaluation of organizational lifecycle-related assurance
254 requirements for device software development. DTSec assurance packages **shall** be
255 defined and included within any Protection Profiles authored under this standard.

256
257 An additional approach to evaluation efficiency that should be considered in an
258 evaluation program is a vendor's ability to demonstrate consistent evaluation
259 success. For example, if a vendor successfully passes an evaluation and therefore
260 certifies a product against a DTSec PP/ST, then subsequent versions of similar
261 products, wherein the vendor asserts compliance to all requirements of the ST, may
262 claim a de-facto certification subject to randomized auditing by DWG and/or its
263 appointed subcontractor.

264
265 Security evaluation and certification for high-criticality products and components
266 performed under the auspices of this standard **shall** target a custom assurance
267 package that satisfies the aims of protection against moderate to high potential
268 attack threats. The precise selection of custom assurance package depends on
269 numerous factors, including relative criticality, system tolerance to faults, specific
270 selection of assurance requirements, and more. Lower level assurance evaluations
271 **shall** be limited to general-purpose products components not responsible for life-
272 critical functions, or devices that are not exposed to such attack threats (e.g. non-
273 networked devices used only within hospitals).

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

274

275 The primary initial audience for product evaluation is medical device manufacturers
276 and their suppliers, although patients, doctors, regulators, device purchasers, and
277 other stakeholders also will have an interest in the results of such evaluations.
278 While DWG is expected to author PPs for major classes of diabetes-related medical
279 devices with technical community input, suppliers of components that implement a
280 subset of security functions required by these devices, such as SSL protocol, BTLE,
281 and cryptographic libraries, are also encouraged to evaluate and certify these
282 components against custom STs (approved by DWG) so that device manufacturers
283 can efficiently incorporate them into a reduced scope and resource product
284 evaluation. Component STs *shall* be carefully defined so that they use the same
285 assurance level as the devices that will contain them, and functionality claims *shall*
286 be consistent with the relevant parts of the PPs.

287

DRAFT

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

288
289

290 2. ASSURANCE PROGRAM

291

292 While a standardized documentary approach to specification and evaluation of
293 security requirements is important, the actual evaluation of products against these
294 requirements is the cornerstone of DTSec's approach to enhanced cybersecurity
295 assurance. As such, DTSec governs the accreditation of independent testing labs
296 that perform evaluations against this standard and the certification of lab results
297 under this standard.

298 Lab Accreditation

299

300 DWG **shall** publicize a list of independent labs approved by DWG to perform
301 evaluations under DTSec. Labs that wish to provide evaluation services under
302 DTSec must apply and be accepted into the program by DWG.

303

304 Labs approved under DTSec **shall** be accredited against the ISO 17025 lab
305 accreditation standard, under a scope that includes information technology security
306 testing or similar designation. In addition, DWG reserves the right to accept or reject
307 lab applications based on numerous factors, including but not limited to the lab's
308 experience in information technology and vulnerability assessment, the reputation
309 and international acceptance of the lab's ISO 17025 accrediting body, and the lab's
310 prevailing evaluation costs and resource availability.

311

312 Labs approved under DTSec **shall** be competent to perform vulnerability
313 assessment consistent with AVA_VAN¹ requirements at AVA_VAN.4 or higher
314 leveling, as described in ISO 15408 and ISO 18045. In addition, the lab must be
315 capable of handling vulnerability assessment at these levels for a wide range of
316 device software and hardware environments that are typical in the medical device
317 industry. For example, some devices will run on simple microcontrollers with basic
318 operating systems and small applications, while others may include sophisticated
319 web interfaces and general-purpose operating systems and applications. Since such
320 competence may not be included within the scope of the lab's accreditation, the lab
321 must demonstrate its suitability during the application process to DWG. It is the
322 responsibility of DWG to mandate and take reasonable steps to maximize
323 effectiveness and consistency of AVA_VAN implementations across labs; however,
324 DWG recognizes that vulnerability assessment is a function of evaluator skill and
325 time invested as well as specific device characteristics and that perfect consistency

¹ These are vulnerability analyses under the Common Criteria.

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

326 (even with the same lab across different devices) is not realistic. DWG requires that
327 labs document their assessment work and make itself available to auditing and
328 informal observation during evaluations by the DWG. Despite the acknowledged
329 challenges in the world of consistent security evaluation, this difficulty should never
330 be used as an excuse to lower the assurance bar for DTSec.

331 **Product Certification**

332

333 If a product successfully passes evaluation by a DTSec-approved lab, the lab must
334 submit an Evaluation Technical Report to DWG. The report must provide enough
335 detail to satisfy DWG that the evaluation of the product against the ST was
336 performed to a high standard, especially with respect to AVA_VAN vulnerability
337 assessment. A product **shall** not be considered certified under DTSec until the
338 evaluation report is formally accepted by DWG and the product listed under the
339 DTSec evaluated products list.

340 **Evaluated Products List**

341

342 Any products that have successfully passed an evaluation under DTSec and whose
343 evaluation results have been certified by DWG shall be listed under a publicly
344 disclosed DTSec evaluated products list. However, if certified products are
345 subsequently reported to contain vulnerabilities that conflict with the applicable ST
346 requirements, DWG reserves the right to remove those products from the evaluated
347 products list until the vulnerabilities are remediated. DWG reserves the right to
348 remove products from the evaluated products list if they suffer from a large volume
349 of recurring vulnerabilities, even if all reported vulnerabilities have been
350 remediated; similarly, a lab that has successfully evaluated a product that suffers
351 from such recurring vulnerabilities may be subject to removal from the list of
352 approved labs.

353 **Protection Profile and Security Target Approval**

354

355 DWG **shall** author and publish PPs and incorporate public review and feedback
356 prior to their formal acceptance and use to derive any STs.

357

358 An ST **shall** be used for any evaluations performed under DTSec. Public review and
359 formal publication under DTSec of STs are encouraged but not required. An ST
360 **shall** be reviewed and approved by DWG before it may be used in any evaluation
361 under DTSec.

362 **Assurance Maintenance Program**

363

364 When a product developer wishes to gain reuse of a product certification for new
365 versions of the product (hardware and/or software changes), then the developer

This is a PRELIMINARY DRAFT STANDARD and is not intended, nor should it be interpreted, to have any legal effect. This DRAFT reflects the input of Members of the Steering Committee and the Diabetes Technology Society and will be circulated for wider comment following additional internal revisions

366 must submit an assurance maintenance request form, which documents the
367 differences between the certified product and the new, modified product. If the
368 changes are sufficiently minor, DWG may accept the form without any further
369 actions and simply append the new product version information to the applicable
370 entry in the evaluated products list.

371
372 Product developers should notify DWG of high severity vulnerabilities that could be
373 exploited to subvert the asserted security functional requirements in evaluated
374 products. Developers should include a plan to mitigate such problems. If such
375 vulnerabilities, whether reported by developers or third parties, are not adequately
376 and promptly mitigated, DWG reserves the right to remove the product from the
377 evaluated products list. Because the overall impact of vulnerabilities and their
378 potential mitigations in specific products vary greatly, this standard does not
379 include guidance for when DWG may take this action. DWG would consider the
380 perspective of all stakeholders, including developers, regulators, patients, and
381 caregivers.

382
383 DWG reserves the right to institute random audits of the developer by DWG
384 personnel and/or DTSec-approved labs in order to obtain assurance that the new
385 product satisfies the original requirements documented in the applicable ST or in an
386 approved ST that has minor revisions from an ST that was previously applied in a
387 full evaluation of the earlier revision product. Such audits aim to sample
388 requirements compliance and require a small percentage of the cost and time of a
389 full evaluation. If a product developer cannot support the audit activities for any
390 reason or if the changes documented in the assurance maintenance request form are
391 deemed sufficiently major by DWG, then DWG reserves the right to require a full
392 revalidation of the new product. DWG and its accredited labs will enter into
393 agreements as needed in order to meet confidentiality requirements of vendors
394 bringing their products into evaluation against this standard.

395
396 This standard does not stipulate a lifetime or expiration for product evaluations; a
397 product evaluation shall remain in effect as long as it continues to meet the
398 assurance maintenance requirements defined herein.
399